在接入服务器上配置基本AAA

目录

简介

本文档介绍如何在采用Radius或TACACS+协议的思科路由器上配置身份验证、授权和记帐(AAA)。

先决条件

要求

本文档没有任何特定的要求。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

使用的组件

本文档中的信息基于Cisco IOS®软件版本12主行。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

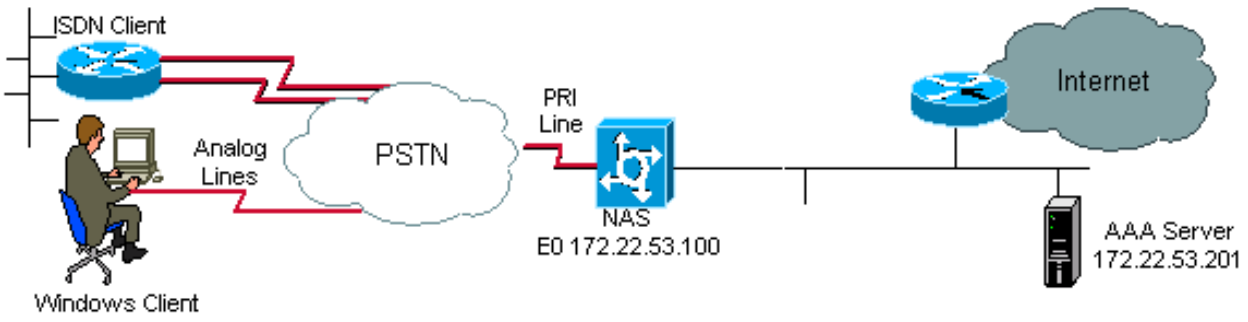
背景信息

本文档介绍如何在采用Radius或TACACS+协议的思科路由器上配置身份验证、授权和记帐(AAA)。本文档的目标不是涵盖所有的 AAA 功能，而是对主要的命令加以介绍并提供一些示例和指南。

> **注意**：在继续进行Cisco IOS配置之前，请阅读有关AAA常规配置的部分。否则可能会导致配置错误和随后的锁定。

有关详细信息，请参阅身份验证、授权和记帐配置指南。

网络图



网络图

一般 AAA 配置

Enable AAA

要启用 AAA，需要在全局配置模式下配置 **aaa new-model 命令。**

注意：在该命令启用前，其他所有 AAA 命令都是隐藏的。

警告：aaa new-model 命令立即对所有线路和接口（控制台线路 line con 0 除外）应用本地身份验证。 如果在启用此命令后打开了到路由器的telnet会话（或者如果连接超时且必须重新连接），则必须使用路由器的本地数据库对用户进行身份验证。建议在启动AAA配置之前在接入服务器上定义用户名和密码，这样就不会锁定路由器。请参见下一个代码示例。

```
Router(config)#username xxx password yyy
```

提示：配置AAA命令之前， save 您的配置。也可以 save 仅在完成AAA配置（并确信该配置能正常工作）后再次进行配置。 这允许您从意外锁定中恢复，因为您可以在重新加载路由器时回滚任何更改。

指定外部AAA服务器

在全局配置模式下，定义与 AAA 一起使用的安全协议（Radius 和 TACACS+）。 如果您不想使用这两种协议，也可以使用路由器上的本地数据库。

如果使用TACACS+，请使用**tacacs-server host** <AAA服务器的IP地址> <key>命令。

如果使用Radius，请使用 **radius-server host <IP address of the AAA server> <key>** 命令。

AAA 服务器配置

在AAA服务器上，配置以下参数：

- 接入服务器的名称。
- 接入服务器用来与 AAA 服务器通信的 IP 地址。**注意：**如果两台设备位于同一个以太网络中，则默认情况下，接入服务器在发出AAA数据包时使用以太网接口上定义的IP地址。当路由器有多个接口（因此有多个地址）时，这个问题就很重要。
- 在接入服务器中配置的完全一样的密钥 **<key>。注意：**密钥的名称区分大小写。
- 接入服务器使用的协议（TACACS+ 或 Radius）。

有关配置上述参数的确切过程，请参阅AAA服务器文档。如果AAA服务器配置不正确，则AAA服务器可以忽略来自NAS的AAA请求，并且连接可能会失败。

AAA 服务器必须拥有一个接入服务器可到达的 IP 地址（执行 **ping 测试可验证连接）。**

身份验证配置

身份验证是在允许用户访问网络和网络服务之前先对其进行验证（通过授权进行检验）。

要配置 AAA 身份验证，请执行以下步骤：

1. 首先，（在全局配置模式下）定义包含身份验证方法的命名列表。
2. （在接口配置模式下）将此列表应用于一个或多个接口。

唯一的例外是默认方法列表(名为**default**)。 默认方法列表自动应用于所有接口，但那些拥有明确定义的命名方法列表的接口除外。定义的方法列表将覆盖默认方法列表。

这些身份验证示例使用Radius、登录和点对点协议(PPP)身份验证来解释方法和命名列表等概念。在所有示例中，均可使用 TACACS+ 替代 Radius 或本地身份验证。

Cisco IOS 软件使用所列出的第一种方法对用户进行身份验证。如果此方法未能响应（通过 ERROR 表明），Cisco IOS 软件将选择方法列表中列出的下一种身份验证方法。此过程将持续下去，直到通过列出的某个验证方法进行了成功的通信或者尝试完列表中定义的所有方法为止。

一定要注意，仅当通过前一种方法未获得任何响应时，Cisco IOS 软件才尝试使用下一种列出的认证方法进行认证。如果身份验证在此循环中的任何时刻失败，即如果AAA服务器或本地用户名数据库响应拒绝用户访问（由FAIL指示），则身份验证过程将停止，并且不会尝试任何其他身份验证方法。

要允许用户身份验证，必须在 AAA 服务器上配置用户名和口令。

登录认证

您可以使用 aaa authentication login 命令，对希望拥有用于接入服务器（tty、vty、控制台和 aux）的 EXEC 访问权限的用户进行身份验证。

示例 1：使用Radius然后使用Local的EXEC访问

```
Router(config)#aaa authentication login default group radius local
```

在上一个命令中：

- 命名列表是默认的列表 (default)。
- 有两种身份验证方法（group radius 和 local）。

所有用户都使用Radius服务器（第一种方法）进行身份验证。 如果Radius服务器没有响应，则使用路由器本地数据库（第二种方法）。 对于本地身份验证，需要定义用户名和口令：

```
Router(config)#username xxx password yyy
```

由于使用 aaa authentication login命令中的列表默认值，因此登录身份验证自动应用于所有登录连接（例如tty、vty、控制台和aux）。

> **注意：**如果没有IP连接、访问服务器未在AAA服务器上正确定义或者访问服务器上未正确定义AAA服务器，则服务器（Radius或TACACS+）无法回复访问服务器发送的aaa authentication请求。

> **注意：**如果使用上一个示例，但不使用 local关键字，则结果为：

```
Router(config)#aaa authentication login default group radius
```

> **注意：**如果AAA服务器没有回复身份验证请求，则身份验证失败（因为路由器没有可尝试的备用方法）。

> **注意：** group关键字提供了一种将当前服务器主机分组的方法。此功能使用户可从配置的服务

器主机当中选择一部分主机，将其用于某项特定服务。

示例 2：控制台访问与线路口令一起使用

展开示例1中的配置，以便控制台登录仅通过线路con 0上设置的密码进行身份验证。

这样将定义 CONSOLE 列表，然后应用于 line con 0。

配置:

```
Router(config)#aaa authentication login CONSOLE line
```

在上一个命令中：

- 命名列表是 CONSOLE。
- 只有一种身份验证方法 (line)。

创建命名列表（在本例中为CONSOLE）时，必须在行或接口上应用该列表，然后才能执行该列表。这通过 login authentication 指令：

```
Router(config)#line con 0
Router(config-line)#exec-timeout 0 0
Router(config-line)#password cisco
Router(config-line)#login authentication CONSOLE
```

CONSOLE列表会覆盖**line con 0上的默认方法列表**默认值。在line con 0上执行此配置后，您需要输入口令**cisco**才能获得控制台访问权限。tty、vty和aux上仍使用默认列表。

注意：要使用本地用户名和密码对控制台访问进行身份验证，请使用以下代码示例：

```
Router(config)#aaa authentication login CONSOLE local
```

这种情况下，用户名和口令必须在路由器的本地数据库中进行配置。列表也必须应用到线路或接口上。

注意：要无身份验证，请使用下一个代码示例：

```
Router(config)#aaa authentication login CONSOLE none
```

这种情况下，不对获取控制台访问权限这一活动进行身份验证。列表也必须应用到线路或接口上。

示例 3：启用与外部AAA服务器一起使用的模式访问

您可以发起身份验证以便进入启用模式（特权 15）。

配置:

```
Router(config)#aaa authentication enable default group radius enable
```

只能请求密码，用户名为$enab15$。因此，必须在 AAA 服务器上定义用户名 $enab15$。

如果Radius服务器没有应答，则可能必须输入路由器上本地配置的启用密码。

PPP 身份验证

aaa authentication ppp 命令用于针对 PPP 连接进行身份验证。它通常用于对希望通过接入服务器访问互联网或中心办公室的ISDN或模拟远程用户进行身份验证。

示例 1：对所有用户都采用一种 PPP 身份验证方法

接入服务器具有配置为接受PPP拨入客户端的ISDN接口。我们使用**dialer rotary-group 0**，但配置可以在主接口或拨号程序配置文件接口上完成。

配置:

```
Router(config)#aaa authentication ppp default group radius local
```

此命令使用Radius验证所有PPP用户。如果Radius服务器没有应答，则使用本地数据库。

示例 2：与特定列表一起使用的PPP身份验证

要使用命名列表而不是默认列表，请配置以下命令：

```
Router(config)#aaa authentication ppp ISDN_USER group radius

Router(config)#interface dialer 0
Router(config-if)#ppp authentication chap ISDN_USER
```

在本示例中，列表为 ISDN_USER，方法为 Radius。

示例 3：从字符模式会话内部启动 PPP

接入服务器有一个内置调制解调器卡（Mica、Microcom 或 Next Port）。 假设同时配置了**aaa authentication login**和**aaa authentication ppp**命令。

如果调制解调器用户首先使用字符模式exec会话访问路由器（例如，拨号后使用终端窗口），则用户在tty线路上进行身份验证。要启动到数据包模式会话中，用户必须键入 **ppp default 或 ppp。**因为已明确配置 PPP 身份验证（使用 **aaa authentication ppp 命令），所以再次在 PPP 级别对用户进行身份验证。**

要避免第二次身份验证，请使用**if-needed**关键字：

```
Router(config)#aaa authentication login default group radius local
Router(config)#aaa authentication ppp default group radius local if-needed
```

注意：如果客户端直接启动PPP会话，则直接执行PPP身份验证，因为接入服务器没有登录访问。

配置授权

授权是控制用户可执行的操作的流程。

AAA 授权与身份验证的规则相同：

1. 首先，定义包含授权方法的命名列表。
2. 然后，将此列表应用于一个或多个接口（默认方法列表则例外）。
3. 使用所列出的第一种方法。如果此方法未能响应，则使用第二种方法，依此类推。

方法列表特定于所请求的授权类型。本文档重点介绍Exec和网络授权类型。

有关其他授权类型的详细信息，请参阅Cisco IOS安全配置指南。

Exec 授权

aaa authorization exec 命令确定是否允许用户运行 EXEC shell。此工具可以返回用户配置文件信息，例如自动命令信息、空闲超时、会话超时、访问列表和权限以及其他每用户因素。

EXEC 授权只在 vty 和 tty 线路上执行。

下一个示例使用Radius。

示例 1：对所有用户都采用相同的 EXEC 身份验证方法

使用以下内容进行身份验证时：

```
Router(config)#aaa authentication login default group radius local
```

所有要登录访问服务器的用户都必须使用Radius（第一种方法）或本地数据库（第二种方法）进行授权。

配置:

```
Router(config)#aaa authorization exec default group radius local
```

注意：在 AAA 服务器上，必须选择 Service-Type=1 (login)。

注意：在本示例中，如果不包括 **local**关键字，并且AAA服务器没有响应，则无法进行授权，连接可能会失败。

注意：在接下来的示例2和3中，您无需在路由器上添加任何命令。您只需在接入服务器上配置配置文件。

示例 2：从AAA服务器分配Exec权限级别

根据示例1，在AAA服务器上配置下一个思科AV对，以便用户可以登录接入服务器并直接进入启用模式：

```
shell:priv-lvl=15
```

用户现在可以直接进入启用模式。

注意：如果第一种方法未能响应，则使用本地数据库。但是，用户无法直接进入启用模式，但必须输入enable命令并提供**enable**口令。

示例 3：从AAA服务器分配空闲超时

要配置空闲超时（以便在空闲超时后没有流量时会话断开），请使用IETF Radius属性28:用户配置文件下的Idle-Timeout。

网络授权

此 **aaa authorization network** 命令对所有网络相关的服务请求（例如PPP、SLIP和ARAP）运行授权。本节重点介绍最常用的PPP。

AAA 服务器检查客户端发起的 PPP 会话是否得到了允许。而且，客户端可以请求 PPP 选项：回拨、压缩、IP 地址等。这些选项必须在 AAA 服务器上的用户配置文件中配置。此外，对于特定客户端，AAA配置文件可以包含空闲超时、访问列表和其他每用户属性，这些属性可以由Cisco IOS软件下载并应用于此客户端。

下一个示例显示使用Radius的授权。

示例 1：对所有用户都采用相同的网络授权方法

接入服务器用于接受PPP拨入连接。

用户通过身份验证（如先前配置）：

```
Router(config)#aaa authentication ppp default group radius local
```

使用下一命令授权用户：

```
Router(config)#aaa authorization network default group radius local
```

注意：在 AAA 服务器上配置： **Service-Type=7**(framed)和**Framed-Protocol=PPP**。

示例 2：应用用户特定属性

您可以使用AAA服务器为每个用户分配属性，例如IP地址、回拨号码、拨号程序空闲超时值或访问列表等。在该实施过程中，NAS 从 AAA 服务器用户配置文件中下载相应的属性。

示例 3：使用特定列表的 PPP 授权

与身份验证类似，配置列表名称而不是默认名称：

```
Router(config)#aaa authorization network ISDN_USER group radius local
```

然后，将此列表应用到接口：

```
Router(config)#interface dialer 0
Router(config-if)#ppp authorization ISDN_USER
```

记帐配置

AAA记帐功能使您能够跟踪用户访问的服务及其使用的网络资源量。

AAA 记帐的规则与身份验证及授权的规则相同：

1. 首先，必须定义包含记帐方法的命名列表。
2. 然后，将此列表应用于一个或多个接口（默认方法列表则例外）。
3. 使用所列出的第一种方法；如果此方法未能响应，则使用第二种方法，依此类推。

- 网络记帐为所有 PPP、Slip 和 AppleTalk 远程访问协议 (ARAP) 会话提供信息：数据包计数、八位字节计数、会话时间、开始和结束时间。
- EXEC 记帐提供关于网络接入服务器的用户 EXEC 终端会话（例如 Telnet 会话）的信息：会话时间、开始和结束时间。

以下示例重点介绍如何将信息发送到AAA服务器。

记帐配置示例

示例 1：生成开始和停止记帐记录

对于每个拨入PPP会话，在客户端通过身份验证之后，并在断开之后使用关键字**start-stop**将记帐信息发送到AAA服务器。

```
Router(config)#aaa accounting network default start-stop group radius local
```

示例 2：仅生成停止记帐记录

如果必须在客户端断开连接后发送记帐信息，请使用关键字 **stop**并配置下一行：

```
Router(config)#aaa accounting network default stop group radius local
```

示例3：生成身份验证和协商失败的资源记录

此时，AAA 记帐为已通过用户身份验证的呼叫提供开始和结束记录支持。

如果身份验证或 PPP 协商失败，则没有身份验证记录。

解决方法是使用 AAA 资源失败结束记帐：

```
Router(config)#aaa accounting send stop-record authentication failure
```

此时将发送结束记录到 AAA 服务器上。

示例 4：启用完整资源记帐

要启用完全资源记帐（在呼叫建立时生成开始记录并在呼叫终止时生成结束记录），请进行如下配置：

```
Router(config)#aaa accounting resource start-stop
```

此命令是在 Cisco IOS 软件版本 12.1(3)T 中引入的。

凭借此命令，呼叫建立和呼叫断开的“开始-停止”记帐记录可对资源与设备的连接进度进行跟踪。独立的用户身份验证“开始-停止”记帐记录将跟踪用户管理进度。这两组记帐记录与呼叫的唯一会话ID相互关联。

相关信息

- 技术支持 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。